Solutions Exercise sheet 2

1. Decide whether the following polynomials are irreducible in $\mathbb{Q}[X]$.

(a) $X^3 - 3X^2 - 8$

(b) $2X^{10} - 25X^3 + 10X + 30$

(c) $2X^3 + X^2 + 2X + 2$

(d) $X^4 + X^2 + 1$

Solution:

(a) We will show that the polynomial is irreducible. If $f(X) := X^3 - 3X^2 - 8$ is reducible in $\mathbb{Z}[X]$, then it must then have a linear factor $X - a$ in $\mathbb{Z}[X]$ with a a divisor of 8, which are $\pm 1, \pm 2 \pm 4 \pm 8$. Checking the value at all these points we see that none of them is a zero of the polynomial. Therefore f is irreducible in $\mathbb{Z}[X]$, so by Gauss's lemma f is also irreducible in $\mathbb{Q}[X]$.

(b) We will use Eisenstein's criteria with $p = 5$: note that p divides all the lower coefficients, $-25, 10$ and 30, but $p \nmid 2$ and $p^2 \nmid 30$. Hence the polynomial is irreducible.

(c) In $\mathbb{Z}/3\mathbb{Z}$ the polynomial is again congruent to $\overline{f}(X) = \overline{2}x^3 + x^2 + \overline{2}x + \overline{2}$, and if it is reducible, then it must have a linear factor, since it has degree 3. We can check:

$$\overline{f}(\overline{0}) = \overline{2}$$
$$\overline{f}(\overline{1}) = \overline{1}$$
$$\overline{f}(\overline{2}) = \overline{2}$$

so f is irreducible in $\mathbb{Q}[X]$.

(d) This is reducible:

$$X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1).$$

2. Consider the ring $R = \mathbb{Z}[X]/(X^2 + 5)$.

(a) Show that R is an integral domain.

(b) Show that R is not a unique factorization domain.

Solution: (a) The polynomial $X^2 + 5$ has no roots in $\mathbb{Z}$, so it is irreducible in $\mathbb{Z}[X]$. Since $\mathbb{Z}$ is a unique factorization domain, we have that $\mathbb{Z}[X]$ is a unique factorization domain as well. Hence $X^2 + 5$ is prime. Hence R is an integral domain.

(b) By the First isomorphism theorem, we have that $R \cong \mathbb{Z}[\sqrt{-5}]$. Also, note that $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$. We can define a norm function on $\mathbb{Z}[\sqrt{-5}]$ as

$$N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geqslant 0},\ a + b\sqrt{-5} \mapsto (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Similarly as in Exercise sheet 1, Exercise 3 (c), we can see that N is multiplicative and $s \in \mathbb{Z}[\sqrt{-5}]^* \iff N(s) = 1$.

Claim: The element 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Suppose there exist $a, b, c, d \in \mathbb{Z}$ with

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Taking the norm N on both sides gives

$$4 = (a^2 + 5b^2)(c^2 + 5d^2),$$

which means $a^2 + 5b^2 \in \{1, 2, 4\}$. If $a^2 + 5b^2 = 1$, then $a = \pm 1$ and $b = 0$, which means $a + b\sqrt{-5} = \pm 1$ which is a unit, and we are done. If $a^2 + 5b^2 = 4$, then $a = \pm 2$ and $b = 0$ which means

$$c + \sqrt{-5}d = \frac{2}{a + \sqrt{-5}b} = \frac{2}{2} = 1,$$

is a unit, which means we're done. Finally, notice that $a^2 + 5b^2 = 2$ had no solutions in $\mathbb{Z}$. Hence 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Now, note that $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but $2 \nmid (1 + \sqrt{-5}), (1 - \sqrt{-5})$. Since, if for example $2 \mid 1 + \sqrt{-5}$, then there exist $a, b \in \mathbb{Z}$ such that $1 + \sqrt{-5} = 2(a + b\sqrt{-5})$, which means $2a = 1$ and $2b = 1$, which again is not solvable in $\mathbb{Z}$. Similarly we can argue for $1 - \sqrt{-5}$.

Hence 2 is not prime, but it is irreducible. Since in a unique factorization domain an element is irreducible if and only if it is prime, we have that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

3. Consider the ring $R := \mathbb{Z}[\sqrt{-2}]$.

(a) Show that R is a Euclidean domain with the norm function

$$N \colon R \to \mathbb{Z}_{\geqslant 0},\ a + b\sqrt{-2} \mapsto a^2 + 2b^2.$$

(b) Show that the norm N is multiplicative and hence if $r \mid s$ in $\mathbb{Z}[\sqrt{-2}]$, then $N(r)$ divides $N(s)$.

(c) Show that the only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

Solution: Let $x, y \in R$ with $y \neq 0$. We can write $\frac{x}{y} = a + b\sqrt{-2}$ with $a, b \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that

$$|a - m| \leqslant \frac{1}{2} \quad \text{and} \quad |b - n| \leqslant \frac{1}{2}$$

and let $q := m + n\sqrt{-2}$ and $r := x - yq$. From our construction we obtain:

$$\left|\frac{x}{y} - q\right|^2 = (a - m)^2 + 2(b - n)^2 \leqslant \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1.$$

Then we have $x = yq + r$ with

$$N(r) = |x - yq|^2 = N(y)\left|\frac{x}{y} - q\right|^2 < N(y).$$

Thus R is a Euclidean domain for the function N.

(b) The field norm N satisfies $N(1) = 1$ and is multiplicative: for all $a = a_1 + a_2\sqrt{-2}, b = b_1 + b_2\sqrt{-2} \in R$, with $a_i, b_j \in \mathbb{Z}$, we have

$$\begin{aligned} N(ab) &= N((a_1b_1 - 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{-2}) \\ &= (a_1b_1 - 2a_2b_2)^2 + 2(a_1b_2 + a_2b_1)^2 \\ &= (a_1^2 + 2a_2^2)(b_1^2 + 2b_2^2) = N(a)N(b). \end{aligned}$$

(c) If $s \in R^\times$ is a unit, then also $s^{-1} \in R^\times$. Hence

$$N(s) \cdot N(s^{-1}) = N(ss^{-1}) = N(1) = 1,$$

and thus $N(s) = 1$.

On the other hand, are ± 1 the only elements $s \in R$ with $N(s) = 1$. Hence

$$s \in R^\times \iff N(s) = 1 \iff s = \pm 1.$$

4. The goal of this exercise is to show that the only integral solutions of the diophantine equation $y^2 = x^3 - 2$ are $(x, y) = (3, 5)$ and $(3, -5)$.

(a) Show that if $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 2$ then x is odd.

(b) Show that if $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 2$ then $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime over $\mathbb{Z}[\sqrt{-2}]$

(c) Write $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$ and use Exercise sheet 1, Question 4 (a) to write $(y + \sqrt{-2}) = (a + b\sqrt{-2})^3$ and conclude that only solutions are $(x, y) = (3, 5)$ and $(3, -5)$.

Solution:

(a) If x is even then $8|x^3$ and hence $y^2 \equiv 6 \mod 8$. But the only squares $\mod 8$ are $0, 1, 4$. Hence x must be odd.

(b) If $d = a + b\sqrt{-2}$ is a divisor of $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ then it also divides the difference $2\sqrt{-2}$. Taking norms and using question 3(b) shows that $N(d)|8$. But $N(d)$ also divides $N(y + \sqrt{-2}) = y^2 + 2 = x^3$. Since x is odd (part (a)), $N(d) = 1$. But then we have $a^2 + 2b^2 = 1$ which has only the solutions $(a, b) = (\pm 1, 0)$.

(c) Suppose $x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$. Then since $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime, using Exercise sheet 1, question 4 (a) we have that for some $a, b \in \mathbb{Z}$

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Hence $y = a(a^2 - 6b^2)$ and $1 = b(3a^2 - 2b^2)$. Using the second equation we have that $b = \pm 1$. If $b = 1$ then $1 = (3a^2 - 2b^2) = 3a^2 - 2$. Hence $a = \pm 1$. Setting $a = \pm 1$ and $b = 1$ in $y = a(a^2 - 6b^2)$ gives $y = \pm 5$ and $x^3 = y^2 + 2 = 27$ and hence $x = 3$.

On the other hand if $b = -1$, then $1 = b(3a^2 - 2b^2) = -(3a^2 - 2)$ and we have $3a^2 = 1$ which clearly has no solution in integers. Hence the only solutions to $y^2 = x^3 - 2$ are the ones we found when $b = 1$, namely $(x, y) = (3, \pm 5)$